| | | | |
|---|---|---|---|
| ***Notice of Allowability*** | **Application No.**<br>09/980,873 | **Applicant(s)**<br>FUKUNAKA, TOSHIAKI | |
| | **Examiner**<br>Scott R. Wilson | **Art Unit**<br>2826 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--***
All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to _amendment filed 22 October 2003_.
2. ☒ The allowed claim(s) is/are _1-9_.
3. ☒ The drawings filed on _06 December 2001_ are accepted by the Examiner.
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☒ All b) □ Some* c) □ None of the:

    1. ☒ Certified copies of the priority documents have been received.
    2. □ Certified copies of the priority documents have been received in Application No. _____ .
    3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____.
5. □ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

    (a) □ The translation of the foreign language provisional application has been received.
6. □ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

7. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
8. □ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.

    (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached

    1) □ hereto or 2) □ to Paper No. ____.

    (b) □ including changes required by the proposed drawing correction filed _____, which has been approved by the Examiner.

    (c) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No. _____.

**Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the margin according to 37 CFR 1.121(d).**

9. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1□ Notice of References Cited (PTO-892)
2□ Notice of Draftperson's Patent Drawing Review (PTO-948)
3□ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No. _____
4□ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5□ Notice of Informal Patent Application (PTO-152)
6□ Interview Summary (PTO-413), Paper No._____ .
7☒ Examiner's Amendment/Comment
8□ Examiner's Statement of Reasons for Allowance
9□ Other .

## EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The application has been amended as follows:

**Cancel claims 10-25** as being drawn to an nonelected invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott R. Wilson whose telephone number is 703-308-6557. The examiner can normally be reached on M-F 8:30 - 4:30 Eastern.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on 703-308-6601. The fax phone number for the organization where this application or proceeding is assigned is 703-308-7722.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1782.

srw

Instead of giving a quantum computer algorithm for factoring $n$ directly, we give a quantum computer algorithm for finding the order $r$ of an element $x$ in the multiplicative group (mod $n$); that is, the least integer $r$ such that $x^r \equiv 1 \pmod n$. It is known that using randomization, factorization can be reduced to finding the order of an element [Miller 1976]; we now briefly give this reduction.

To find a factor of an odd number $n$, given a method for computing the order $r$ of $x$, choose a random $x \pmod n$, find its order $r$, and compute $\gcd(x^{r/2}-1, n)$. Here, $\gcd(a,b)$ is the greatest common divisor of $a$ and $b$, i.e., the largest integer that divides both $a$ and $b$. The Euclidean algorithm [Knuth 1981] can be used to compute $\gcd(a,b)$ in polynomial time. Since $(x^{r/2}-1)(x^{r/2}+1) = x^r - 1 \equiv 0 \pmod n$, the numbers $\gcd(x^{r/2}+1, n)$ and $\gcd(x^{r/2}-1, n)$ will be two factors of $n$. This procedure fails only if $r$ is odd, in which case $r/2$ is not integral, or if $x^{r/2} \equiv -1 \pmod n$, in which case the procedure yields the trivial factors 1 and $n$. Using this criterion, it can be shown that this procedure, when applied to a random $x \pmod n$, yields a non-trivial factor of $n$ with probability at least $1 - 1/2^{k-1}$, where $k$ is the number of distinct odd prime factors of $n$. A brief sketch of the proof of this result follows.

Suppose that $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ is the prime factorization of $n$. Let $r_i$ be the order of $x \pmod{p_i^{\alpha_i}}$. Then $r$ is the least common multiple of all the $r_i$. Consider the largest power of 2 dividing each $r_i$. The algorithm only fails if all of these powers of 2 agree: if they are all 1, then $r$ is odd and $r/2$ does not exist; if they are all equal and larger than 1, then $x^{r/2} \equiv -1 \pmod{p_i^{\alpha_i}}$ for every $i$, so $x^{r/2} \equiv -1 \pmod n$. By the Chinese remainder theorem [Knuth 1981, Hardy and Wright 1979, Theorem 121], choosing an $x \pmod n$ at random is the same as choosing for each $i$ a number $x_i \pmod{p_i^{\alpha_i}}$ at random, where $x \equiv x_i \pmod{p_i^{\alpha_i}}$. The multiplicative group $\pmod{p^\alpha}$ for any odd prime power $p^\alpha$ is cyclic [Knuth 1981], so for the odd prime power $p_i^{\alpha_i}$, the probability is at most 1/2 of choosing an $x_i$ having a particular power of two as the largest divisor of its order $r_i$. Thus each of these powers of 2 has at most a 50% probability of agreeing with the previous ones, so all $k$ of them agree with probability at most $1/2^{k-1}$. There is thus at least a $1 - 1/2^{k-1}$ probability that the $x$ we choose is good. This argument shows the scheme will work as long as $n$ is odd and not a prime power; finding a factor of even numbers and of prime powers can be done efficiently with classical methods.

We now describe the algorithm for finding the order of $x \pmod n$ on a quantum computer. This algorithm will use two quantum registers which hold integers represented in binary. There will also be some amount of workspace. This workspace gets reset to 0 after each subroutine of our algorithm, so we will not include it when we write down the state of our machine.

Given $x$ and $n$, to find the order of $x$, i.e., the least $r$ such that $x^r \equiv 1 \pmod n$, we do the following. First, we find $q$, the power of 2 with $n^2 \le q < 2n^2$. We will not include $n$, $x$, or $q$ when we write down the state of our machine, because we never change these values. In a quantum gate array we need not even keep these values in memory, as they can be built into the structure of the gate array.

Next, we put the first register in the uniform superposition of states representing numbers $a \pmod q$. This leaves our machine in state

$$\frac{1}{q^{1/2}} \sum_{a=0}^{q-1} |a\rangle|0\rangle. \tag{5.1}$$

This step is relatively easy, since all it entails is putting each bit in the first register into the superposition $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.